(12) UK Patent Application (19) GB (11) 2 277 814 (13) A
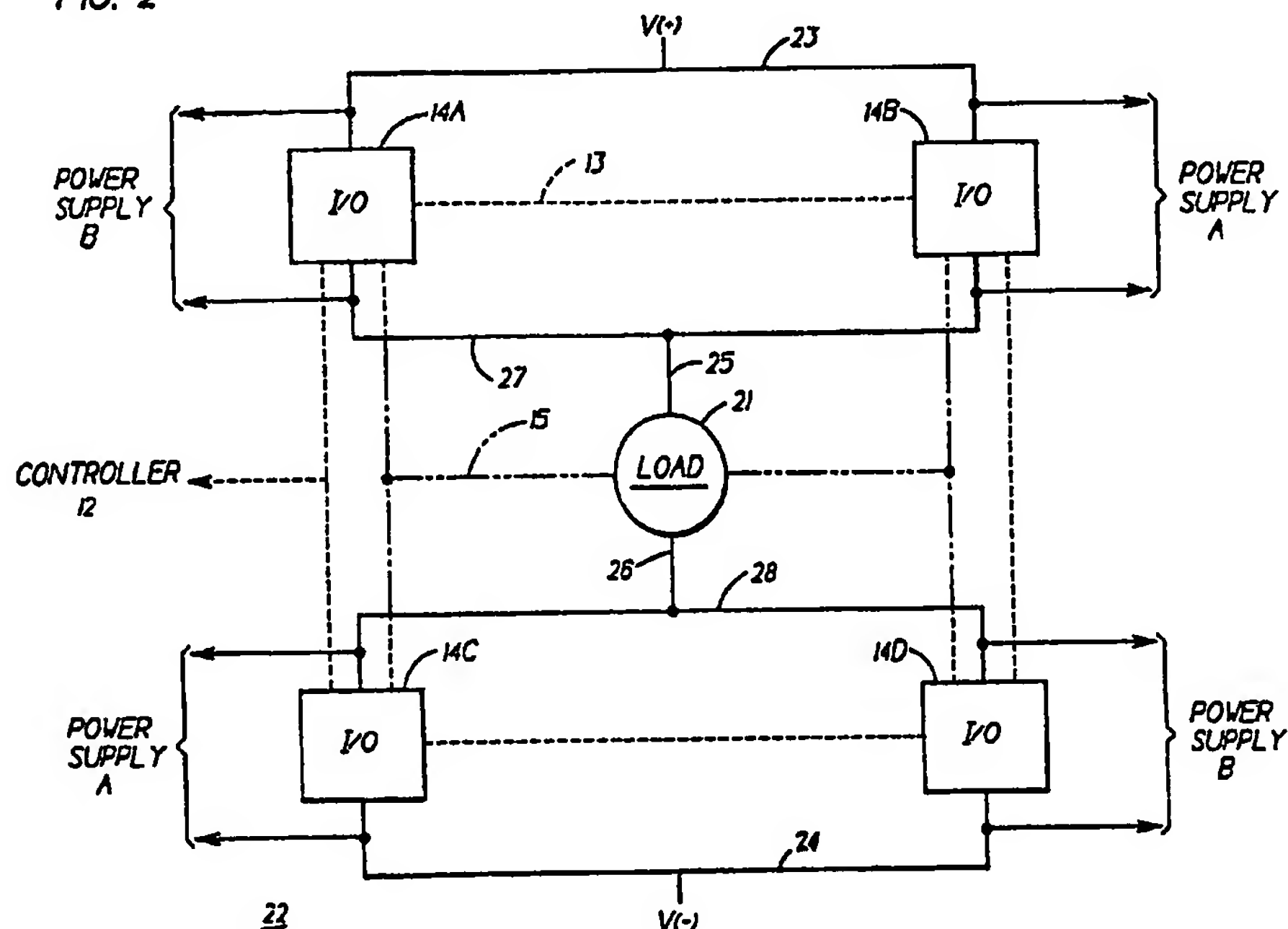
(54) Fault tolerant programmable logic controller

(57)   In a fault tolerant PLC including a CPU and a controller 12, a pair of first I/O modules 14A, 14B are connected between a positive power bus V(+) and the load 21 and a pair of second I/O modules 14C, 14D are connected between the negative power bus (V-) and the load 21. Redundancy is thus provided so that power to the load is not disconnected upon failure of one of the I/O modules on either side of the load.

Algorithms allowing continuous fault checking within any of the I/O modules with either the power off (figure 3) or power on (figure 4) are also disclosed.
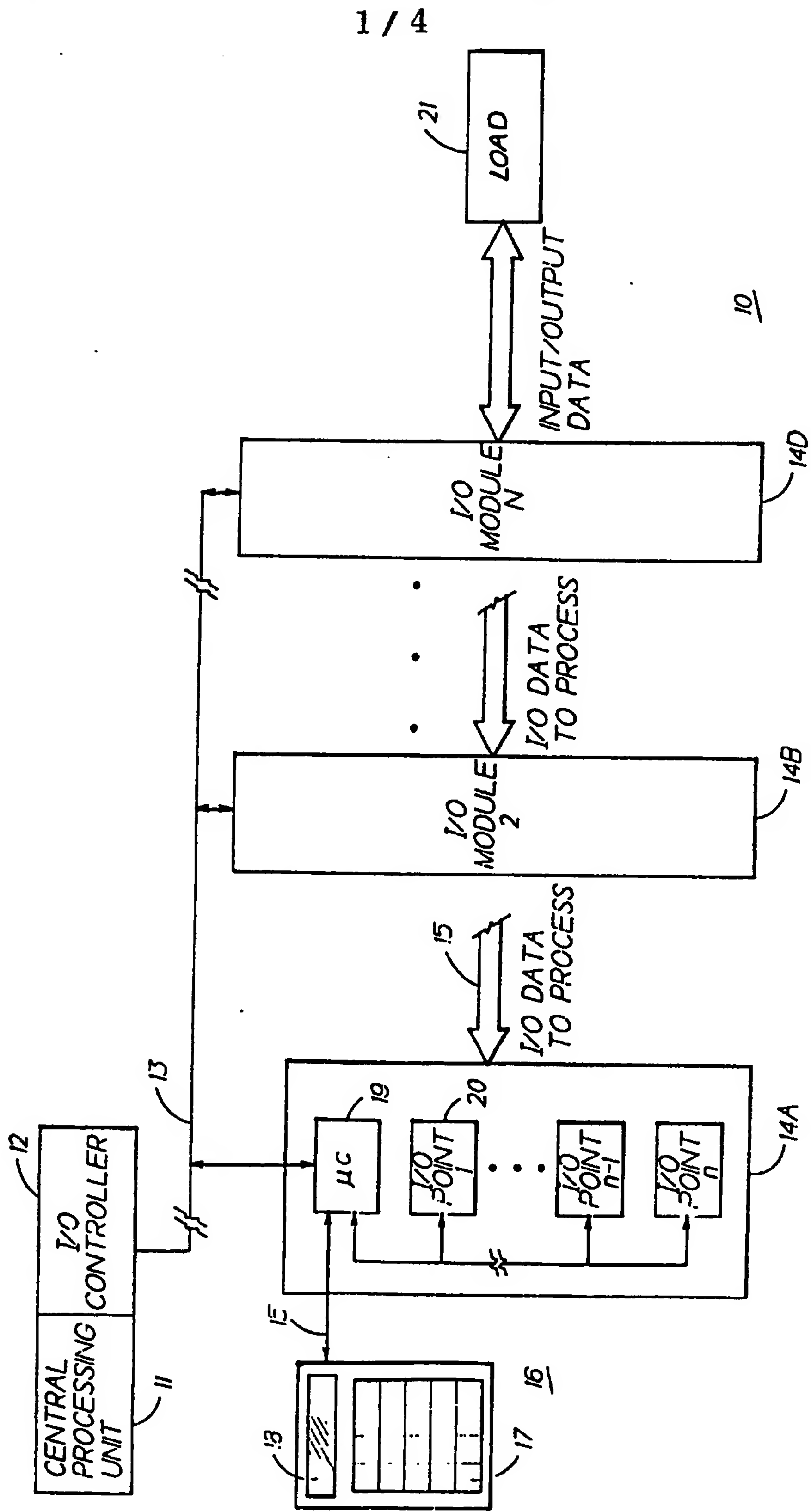
Separate power supplies A and B to the two I/O modules on the same side of the load can be provided so that power is still supplied to the load even if the power supply to one of the modules fails.

FIG. 2

GB 2 277 814 A

FIG. 1
(Prior Art)

FIG. 2

FIG. 3

```
30 ── BEGIN

31 ──  V
     ACROSS ──N──  REPORT   ──32
     A•B ?            FAULT

       Y

33 ──  CLOSE
         C

34 ──  PULSE
         A

35 ──    I
       THRU  ──N──  REPORT A   ──36
        A ?          FAULTED

        Y

37 ──    V
       ACROSS ──Y──  REPORT A   ──38
        A ?           FAULTED

        N

39 ──  PULSE
         B

40 ──    I
       THRU  ──N──  REPORT B   ──41
        B ?          FAULTED

        Y

42 ──    V
       ACROSS ──Y──  REPORT B   ──43
        B ?           FAULTED

        N
```

```
44 ──    V
       ACROSS ──N──  REPORT   ──45
        C•D ?         FAULTED

        Y

46 ──  CLOSE
         A

47 ──  PULSE
         C

48 ──    I
       THRU  ──N──  REPORT C   ──49
        C ?          FAULTED

        Y

50 ──    V
       ACROSS ──Y──  REPORT C   ──51
        C ?           FAULTED

        N

52 ──  PULSE
         D

53 ──    I
       THRU  ──N──  REPORT D   ──54
        D ?          FAULTED

        Y

55 ──    V
       ACROSS ──Y──  REPORT D   ──56
        D ?           FAULTED

        N

       END
```

57 ── STOP
      TEST

29

FIG. 4

BEGIN — 58

I A/B ? — 59 → N → REPORT FAULT — 60

Y

PULSE A — 61

V ACROSS A ? — 62 → Y → REPORT B FAULTED — 63

N

PULSE B — 64

V ACROSS B ? — 65 → Y → REPORT A FAULTED — 66

N

OPEN A — 67

PULSE B — 68

V ACROSS B ? — 69 → N → REPORT A FAULTED — 70

Y

CLOSE A — 71

OPEN B — 72

PULSE A — 73

V ACROSS A ? — 74 → N → REPORT B FAULTED — 75

95

I C/D ? — 77 → N → REPORT FAULT — 78

Y

PULSE C — 79

V ACROSS C ? — 80 → Y → REPORT D FAULTED — 81

N

PULSE D — 82

V ACROSS D ? — 83 → Y → REPORT C FAULTED — 84

N

OPEN C — 85

PULSE D — 86

V ACROSS D ? — 87 → N → REPORT C FAULTED — 88

Y

CLOSE C — 89

OPEN D — 90

PULSE C — 91

V ACROSS C — 92 → N → REPORT D FAULTED — 93

Y

END

STOP TEST — 94
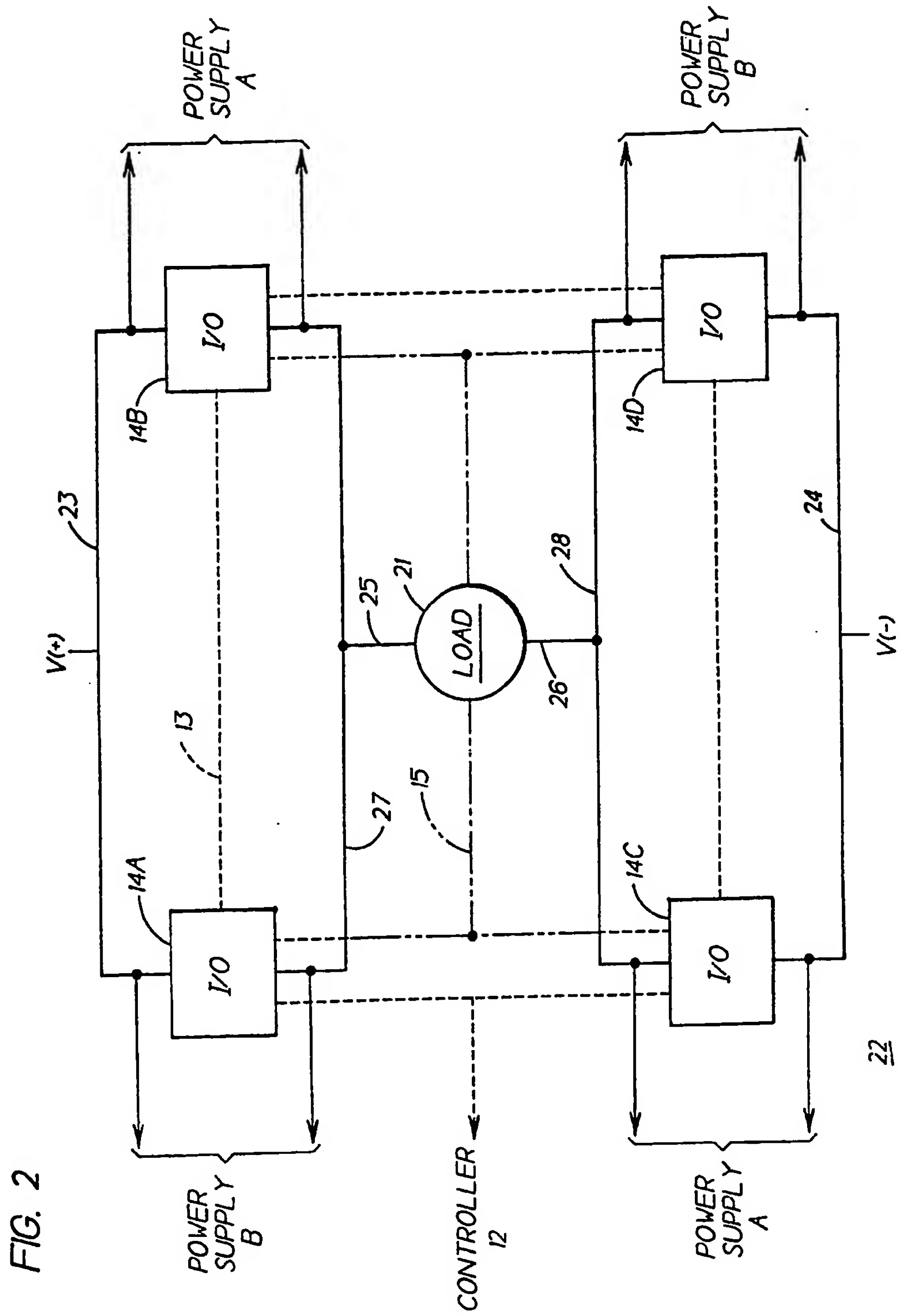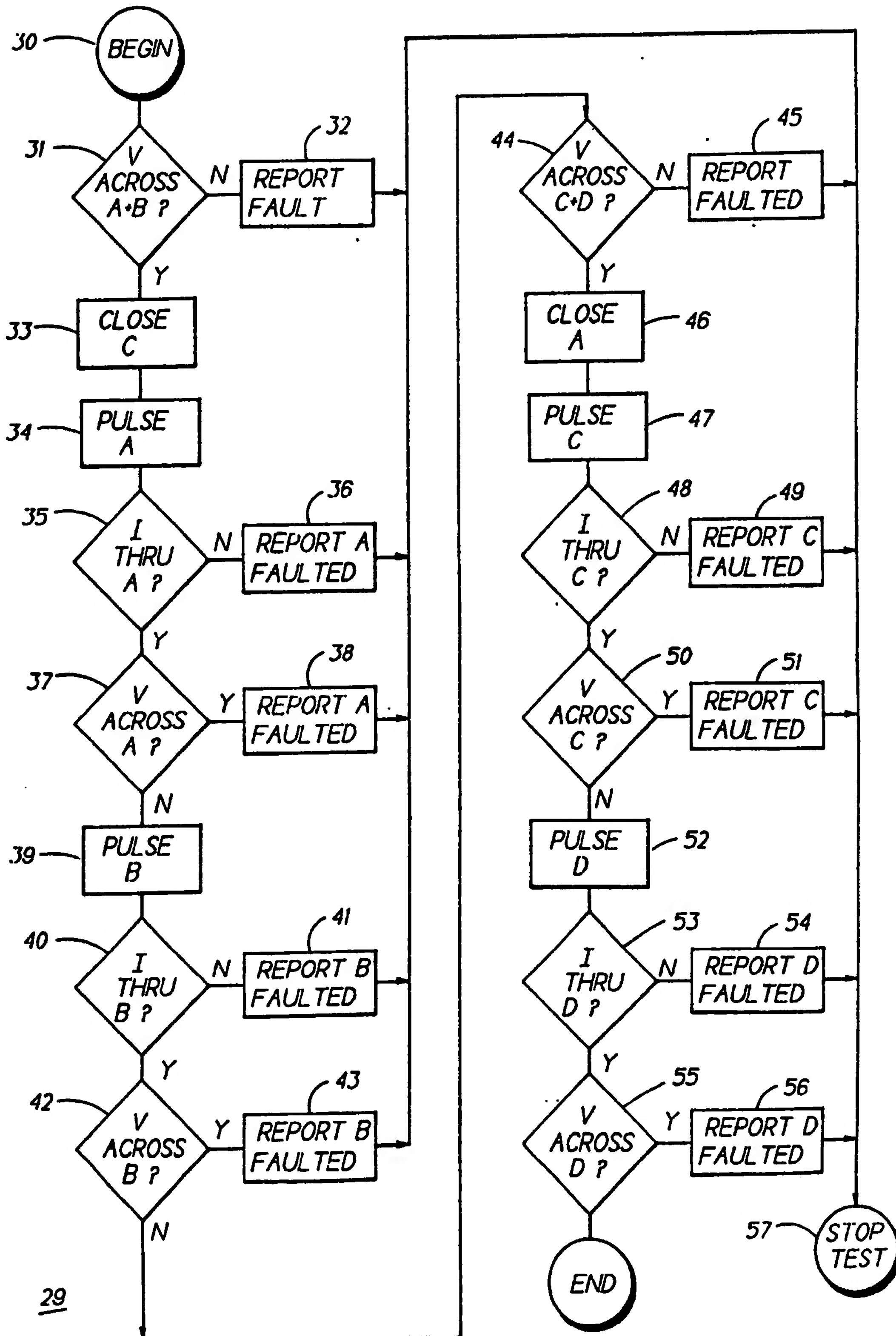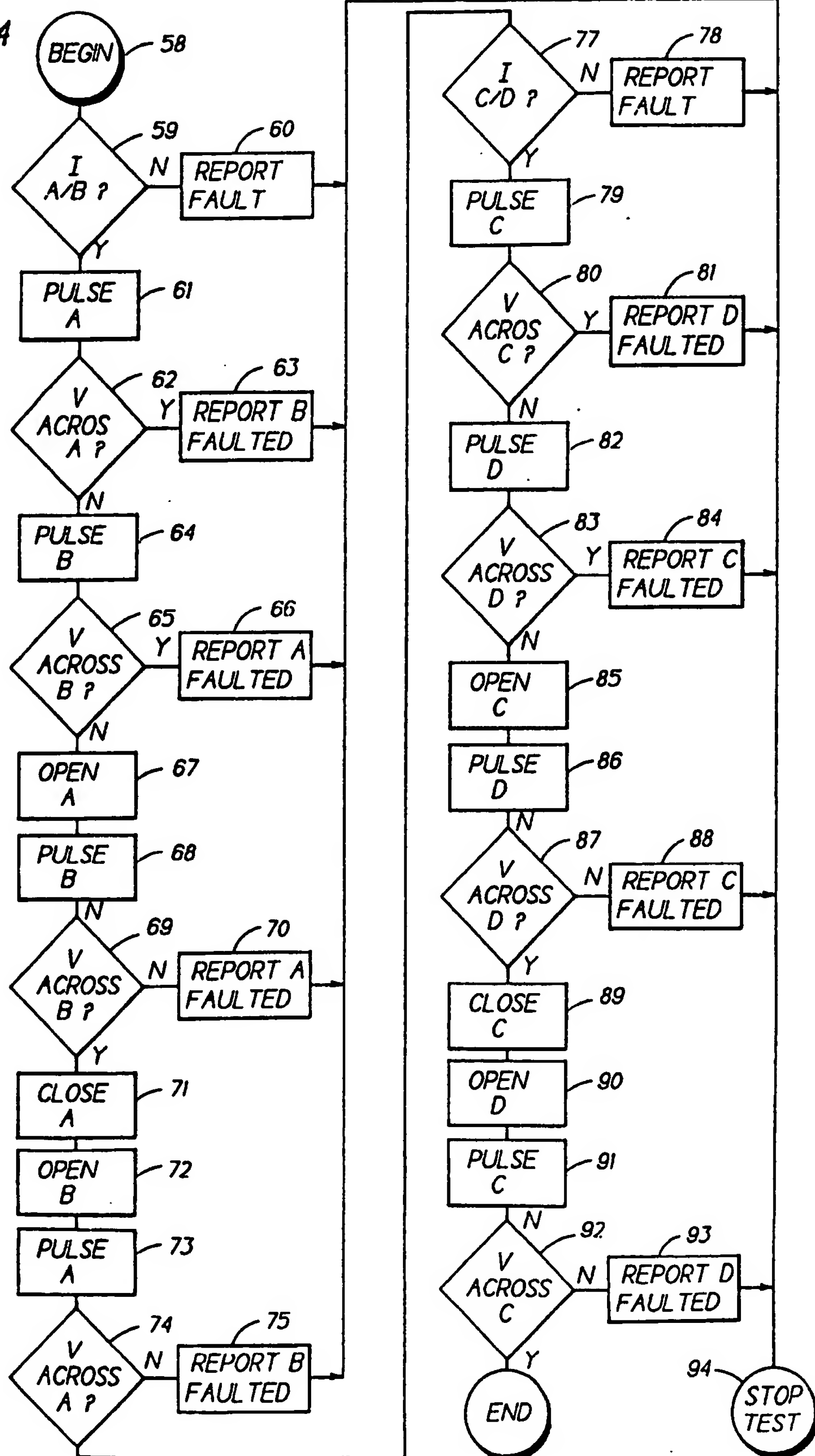
FAULT TOLERANT PROGRAMMABLE CONTROLLER

BACKGROUND OF THE INVENTION

Process control with a programmable
controller involves the acquisition of input
signals from various process sensors and the

5   provision of output signals to controlled elements
of the process. The process is thus controlled as a
function of a stored program and of process
conditions as reported by the sensors. Numerous and
diverse processes are, of course, subject to such

10   control, and sequential operation of industrial
processes, conveyor systems, and chemical,
petroleum, and metallurgical processes may all, for
example, be advantageously controlled by
programmable controllers.

15   Programmable logic controllers (hereinafter
"PLC") comprise a central processing unit (CPU)
made up, broadly, of a data processor for executing
the stored program, a memory unit of sufficient
size to store the program and the data relating to

20   the status of the inputs and outputs, and one or
more power supplies. In addition, an input/output
module provides the interface between the central
processing unit and the input devices and
controlled elements of the process being

25   controlled. U.S. Pat. No. 4,293,924 describes one
such module.

When such PLCS are used with sensitive
equipment such as offshore oil rigs, medical
equipment, nuclear equipment and the like,

30   supplemental circuits are required to insure that

the associated equipment remains operational when
faults may have occurred within any of the modules
associated with the PLCS. So-called "fault
tolerant" operation is described within U.S.

5   Patents 4,868,826 and 4,967,347 wherein discrete
circuit components are employed to provide the
fault tolerant operation. U.S. Patent 4,926,281
describes the use of a pair of redundant modules
interconnected by a means of crowbar switches and

10   supplemental logic circuits to achieve a similar
result.

U.S. Patent 4,752,886 describes a method for
on-line testing of the modules associated with a
PLC to insure operability of the associated load in

15   the event of fault occurrence within any of the
modules. Since standard "off-the-shelf" components
are employed, this approach is relatively
inexpensive to implement.

One purpose of this invention accordingly, is

20   to provide complete fault tolerant operation to a
load associated with a PLC without requiring the
supplemental components and associated customized
circuits currently employed within the state-of-the
art of such fault tolerant operations.

25   SUMMARY OF THE INVENTION
A PLC is interconnected with a sensitive load
by means of a multiplicity of standard
off-the-shelf I/O modules to provide fault tolerant
operation at a substantial cost savings. A pair of

30   similar modules are redundantly interconnected
between the line and the load on both sides of the

DC power distribution system. Sampling algorithms within the PLC continuously test the modules for fault occurrence and disconnect the faulted module without interrupting power to the load.

5   BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a simplified block diagram of a PLC system including a plurality of I/O modules in accordance with the prior art;

FIG. 2 is a diagrammatic representation of 10 the redundant interconnection of the modules of Figure 1 with a power source and a load in accordance with the invention;

FIG. 3 is a flow chart representation of the sampling algorithm for the load of Figure 4 in an 15 OFF state; and

FIG. 4 is a flow chart representation of the sampling algorithm for the load of Figure 4 in an ON state.

DESCRIPTION OF THE PREFERRED EMBODIMENT

20   Before describing the invention in detail, it is helpful to review the operation of a PLC such as described within U.S. Patent 4,628,397. The PLC 10 of FIG. 1 includes a central processing unit (CPU) 11, an I/O controller 12, a plurality of I/O 25 modules 14A-14D, and a data bus 13 which inter-connects each module with the I/O controller. These items, exclusive of the CPU, generally comprise the I/O system of the controller. The CPU is substantially of conventional design and may 30 include one or more microprocessors for data

handling and control, plus memory for storage of
operating programs, input/output data, and other
computed, interim, or permanent data for use in
executing the stored programs and for

5   implementation of control. In addition, other
conventional elements, such as power supplies, are
included as necessary to make the CPU fully
functional. The I/O controller 12 provides for
control of information exchanged between the

10   various modules and the CPU.

Each module may be separately located, remote
from the CPU and the I/O controller, and in close
proximity to the process being controlled as
depicted as a load 21, for example. Although only

15   three modules are illustrated, it will be
understood that the actual number may be considera-
bly greater. For example, sixteen separate modules
may be readily accommodated in the system to be de-
scribed herein. Each module is independent of the

20   other and each may be devoted to control of a
process separate from that controlled by all other
modules. The data bus 13 is preferably a serial
link although parallel transmission of signals
between the CPU and the modules may be readily

25   provided. In either case, the modules are connected
to the data bus for communication with the CPU.
The data bus may comprise a twisted pair of
conductors, a coaxial cable, or a fiber optics
cable; all are acceptable depending on such

30   considerations as cost and availability.

Each module includes a microcontroller 19
having an interface port for exchanging information

with the CPU and including an associated memory
(not illustrated) for implementation of a stored
program of operation according to which the various
elements of the modules are controlled and

5   diagnosed for incurred faults; a plurality of
individual I/O points 20, each of which may be
selectably operated either as an input point or as
an output point and each of which interfaces
individually through conductors directly to input

10   or output elements of the controlled process; and a
data bus 15 for interconnecting the I/O points with
the microcontroller. The number of I/O points
depends on practical considerations such as heat
dissipation and the limitations of the microcon-

15   troller. As an example, it has been found quite
practical and convenient to provide sixteen I/O
points per module.

For verifying the integrity and functionality
of the input and output components and for

20   maintenance and troubleshooting, a monitor unit 16
is provided. The monitor is hand-held so that it
can be readily and conveniently moved from one
module to the other. It is adapted for connection
into each module by a cable 15 which includes a

25   connector for mating with another connector affixed
to the module. The monitor includes a keypad 17 and
display 18 to allow the I/O points of the module to
be monitored and controlled and provides a display
of diagnostic information pertaining to the module.

30   Also connected within each module is a
switching circuit (not shown) which interconnects
the I/O points with the associated load 21. A

preferred switching circuit will, in any case,
include a shunt current path including means for
providing a signal indicative of the current to the
load. The switching circuit most preferred is the
5   insulated gate transistor (hereinafter "IGT") which
comprises a power semiconductor device which may be
gated both into and out of conduction. That is, the
IGT may be both turned on and turned off through
its gate terminal. Some versions of the IGT include
10   a current emulation section which is a section of
the IGT provided to carry a proportional fraction
of the total IGT current. The emulation section is
advantageous in that it can be used to monitor the
total current without resort to means for
15   dissipating large circuit currents. A single gate
signal controls current flow both in the main
section of the IGT and in its emulation section.
The insulated. gate transistor is fully described
within the aforementioned U.S. Patent 4,628,397.
20   The fault tolerant circuit 22 according to
the invention is shown in Figure 2 to include a
pair of modules 14A, 14B, interconnecting between
the positive line bus 23 of a DC power distribution
system and the positive load bus 27 that is
25   connected with one side of the associated load 21
by means of the positive power conductor 25. A
similar pair of modules 14C,14D is connected
between the negative line bus 24 of the DC power
system and the negative load bus 28 that is
30   connected with the other side of the load by means
of the negative power conductor 26. Each of the
modules includes an IGT, although not shown,

operates in the manner described within the aforementioned U.S. Patent 4,628,397. To insure provision of operating power to the modules, each module connecting with the same side of the load is

5   connected with a different source of operating power which are indicated as power supply A and power supply B. Either of which could comprise a set of batteries or an auxiliary DC generator. In the event that one of the power supplies fails, at

10 least one pair of modules would be operational to continue to supply power to the load. The provision of the separate power supplies is an important feature of the invention. To distinguish between the positive power conductor 25 connecting with the

15 positive load bus 27 and the negative power conductor 26 connecting with the negative load bus 28, the data bus 13 interconnecting the modules and the controller 12 (Figure 1) is indicated in dashed lines and the data bus 15 interconnecting the

20 modules and the load is indicated in phantom. An additional feature is the redundant arrangement of the modules on both sides of the load to insure that the load remains operational in the event one of the modules on either side of the load should

25 fail.

In further accordance with the invention, the modules are each connected as both Input and Output modules providing information to the load as well as receiving information from the various

30 sensors associated with the load. In the arrangement depicted in Figure 2, modules 14A and 14C are in the ON state wherein their associated

IGTs are turned on and the modules 14B, 14D are in their OFF state with their associated IGTs turned off To insure operability of the associated load in the event that one of the modules or any of
5   their IGTs should fail, the sampling algorithms in Figures 3 and 4 are employed within the CPU 11 of the PLC 10 of Figure 1. Before the load is automatically disconnected from the power supply, both of the modules connected on the same side of
10   the supply bus must indicate a fault.

The algorithms 29 of Figure 3 and 95 of Figure 4 determine the presence or absence of voltage across the associated IGTs as well as the presence of current through the IGTs to indicate
15   whether the IGTs are operational. In the algorithms "A", "B", "C" and "D" represent the IGTs associated within the modules 14A, 14B, 14C and 14D respectively. The algorithm 29 of Figure 3 is designed to test the associated IGTs when the load
20   21 of Figure 2 is de-energized, i.e. "OFF" and the algorithm 95 of Figure 4 is designed to test the associated IGTs when the load is energized, i.e. "ON". The method of pulsing a load to determine the operability of the module components is
25   described within the aforementioned U.S. Patent 4,752,886.

Referring now to Figure 3, a determination is made as to whether there is voltage across A and B (30,31) and if so C is closed (33) and A is pulsed
30   (34). If there is no voltage, a fault is reported to the CPU (32) and the test is stopped (57). A determination is made as to whether there is

current through A (35) and if not, A is reported as
faulted (36) and the test is stopped (57). If
there is current through A , the voltage across A
is measured (37) and A is reported as faulted if
5   such voltage is present (38) and the test is
stopped (57). If there is no voltage across A, B
is pulsed (39) and the current through B is
determined (40). If there is no current, B is
reported as faulted (41) and the test is stopped
10   (57). If there is current through B, the voltage
across B is measured (42) and B is reported as
faulted if there is a voltage across B (43). The
voltage across C and D is next determined (44) and
if there is no voltage, a fault is reported to the
15   CPU (45) and the test is stopped (57). If there is
a voltage across C and D , A is closed (46) and C
is pulsed (47). The current through C is measured
(48) and if no current exists, C is reported as
faulted (49) and the test is stopped (57). The
20   voltage across C is measured (50) and if there is
voltage, C is reported as faulted (51) and the test
is stopped (57). D is then pulsed (52) and the
current through D is measured (53) and if no
current exists, D is reported as faulted (54) and
25   the test is stopped (57). The voltage across D is
measured (55) and if there is voltage, D is
reported as faulted (56) and the test is stopped
(57). If there is no voltage across D, the
sampling is completed for one test cycle.
30   The algorithm 95 for the load in the "ON"
state is depicted in Figure 4 and begins (58) with
a determination as to whether there is current

through either A or B (59) and if not, a fault is reported to the CPU (60) and the test is stopped (94). If there is current, A is pulsed (61), the voltage across A is measured (62) and if there is

5   voltage, B is reported as faulted (63) and the test is stopped (94). If no voltage, B is pulsed (64), the voltage across B is measured (65) and if there is voltage, A is reported faulted (66) and the test is stopped (94). If no voltage, A is opened (67),

10   B is pulsed (68), and the voltage across B is measured (69). No voltage across B results in A reported faulted (70) and the test stopped (94). If there is voltage across B, A is closed (71), B is opened (72) and A is pulsed (73). The voltage

15   across A is measured (74), and if no voltage, B is reported faulted (75), and the test is stopped (94). The current through C or D is measured (77), and if no current, a fault is reported to the CPU (78) and the test is stopped (94). If there is

20   current, C is pulsed (79), and the voltage across C is measured (80). If there is voltage, D is reported as faulted (81) and the test is stopped (94). If there is no voltage, D is pulsed (82) and the voltage across D is measured (83). If there is

25   voltage, C is reported as faulted (84) and the test is stopped (94). If no voltage, C is opened (85) and D is pulsed (86). The voltage across D is measured (87) and if no voltage (88), C is reported as faulted and the test is stopped (94). If there

30   is voltage, C is closed (89), D is opened (90) and C is pulsed (91). The voltage across C is measured (92) and if no voltage, D is reported as faulted

(93) and the test is stopped (94). If there is voltage, the test is ended.

A PLC has herein been described providing fault tolerant operation to an associated load.

5   The PLC is interconnected with the load by means of a plurality of I/O modules wherein one pair of the modules interconnects the load with the positive power bus and a separate pair of the modules interconnects the load with the negative

10   power bus. Sampling algorithms stored in the PLC test the modules continuously to determine whether any of the modules have become faulted.

CLAIMS

1.   A fault tolerant programmable logic
controller comprising:

a central processor unit;
a controller unit operably connected with
5   said processor unit and adapted for providing
output control signals;
a pair of first I/O modules connected with
said controller and receiving said output control
signals, said first modules interconnecting
10   between a positive power bus and a load; and
a pair of second I/O modules connected with
said controller and receiving said output control
signals, said second modules interconnecting
between a negative power bus and said load, whereby
15   said load remains operational upon failure of
either one of said first or second I/O modules.

2.   The fault tolerant programmable logic
controller of claim 1 wherein said first and second
modules include an electronic switch.

3.   The fault tolerant programmable logic
controller of claim 2 wherein said electronic
switch includes means for measuring voltage and
current.

4.   The fault tolerant programmable logic
controller of claim 1 wherein said electronic
switch comprises a transistor.

5. The fault tolerant programmable logic controller of claim 4 wherein said electronic switch comprises an insulated gate transistor.

6. The fault tolerant programmable logic controller of claim 1 wherein said central processor unit is interconnected with said modules by means of a first data bus.

7. The fault tolerant programmable logic controller of claim 1 wherein said modules are interconnected with each other and said load by means of a second data bus.

8. The fault tolerant programmable logic controller of claim 1 wherein said first modules are connected together in parallel.

9. The fault tolerant programmable logic controller of claim 1 wherein said second modules are connected together in parallel.

10. The fault tolerant programmable logic controller of claim 1 wherein one of said first modules is connected to a first power supply and the other of said first modules is connected to a second power supply electrically isolated from said first power supply.

11. The fault tolerant programmable logic controller of claim 1 wherein one of said second modules is connected to a first power supply and the other of said second modules is connected to a

5   second power supply electrically isolated from said first power supply.

12. A method of providing fault tolerant operation to an electric load comprising the steps of:

      providing a programmable logic controller

5   having a central processor unit and a controller unit;

      connecting a plurality of I/O modules between said controller unit and a load each of said modules including an electronic switch;

10   connecting a first pair of said I/O modules between a positive power bus and a positive input to said load; and

      connecting a second pair of said I/O modules between a negative power bus and a negative input

15   to said load.

13. The method of claim 12 including the step of connecting one module from said first pair and one module from said second pair to a first common power supply.

14.   The method of claim 13 including the step of connecting another module from said first pair and another module from said second pair to a second common power supply electrically-isolated from said
5   first power supply.

15.   The method of claim 12 including the steps of measuring current through first electronic switches within said first pair of modules and disconnecting said load when current is absent from both said
5   electronic switches within said first pair.

16.   The method of claim 12 including the steps of measuring current through said second pair of modules and disconnecting said load when current is absent from both said electronic switches within
5   said second pair.

17.   The method of claim 12 including the steps of reporting a fault condition to said central processor when current is applied to one of said first electronic switches and a voltage is detected
5   across said one first electronic switch.

18.   The method of claim 12 including the steps of reporting a fault condition when current is applied to one of said second switches and a voltage is measured across said one second electronic switch.

19.   The method of claim 17 wherein said current is applied to said first electronic switches when said load is energized.

20.   The method of claim 17 wherein said current
is applied to said second electronic switches when
said load is de-energized.

21.   A controller as claimed in claim 1 and substantially
as described with reference to the accompanying drawings.

22.   A method as claimed in claim 12 and substantially as
described with reference to the accompanying drawings.

Relevant Technical Fields (i) UK Cl (Ed.M) G3N (NGK2, NGK2B) (ii) Int Cl (Ed.5) G05B 9/03 AND G06F 11/16 /20 **Databases (see below)** (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii) ONLINE DATABASES: WPI	**Search Examiner** ANDREW BARTLETT **Date of completion of Search** 4 July 1994 Documents considered relevant following a search in respect of Claims :- 1-20

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&:   Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages	Relevant to claim(s)
	NONE FOUND	